

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF MISSOURI**

**Tumey L.L.P.**

**and**

**Tod T. Tumey**

Plaintiffs,

**vs.**

**Mycroft AI Inc.,**

National Registered Agents, Inc  
120 South Central Avenue  
Clayton, MO 63105

**Joshua Montgomery,**

75-1097 Keopu Mauka Dr.  
Holualoa, HI 96725-9622

**and**

**Michael Lewis**

723 Angelus PL,  
Venice, CA 90291-4918

Defendants.

**Case No. 4:21-cv-00113**

**Jury Trial Demanded**

**VERIFIED COMPLAINT**

COME NOW the Plaintiffs Tumey L.L.P. and Tod T. Tumey (“Tumey” and, together with Tumey L.L.P., “Plaintiffs”) and for their Complaint against Defendants Mycroft AI Inc. (“Mycroft”), Joshua Montgomery (“Montgomery”) and Michael Lewis (“Lewis,” and, collectively with Mycroft and Montgomery, “Defendants”), state and allege as follows:

## **INTRODUCTION**

1. By this action, Plaintiffs seeks interim and permanent injunctive relief, damages, and other remedies, as set forth herein, to address malicious and ongoing cyberattacks, harassment, threats, and other damage being inflicted on Plaintiffs by Defendants.

2. Plaintiffs are an attorney and law firm who represent Voice Tech Corporation (“Voice Tech”) in connection with a dispute between Voice Tech and Mycroft arising from Mycroft’s alleged infringement of Voice Tech’s patents.<sup>1</sup> In particular, Plaintiffs represented Voice Tech to initially raise its infringement claim with Mycroft before any suit was filed, and they currently are counsel of record for Voice Tech in multiple pending matters related thereto, including two lawsuits between Voice Tech and Mycroft that are pending before this Court (the “Patent Suits”)<sup>2</sup> and two *inter partes* review proceedings before the Patent Trial and Appeal Board (“PTAB”) involving Voice Tech’s Patents (the “IPR Proceedings”)<sup>3</sup> (collectively, the Patent Suits, IPR Proceedings, and the underlying dispute between Mycroft and Voice Tech regarding the Patents are referred to herein as the “Voice Tech Matters”).

3. As described and shown by the allegations below, in retaliation against Plaintiffs for their representation of Voice Tech, Defendants have undertaken and/or incited a vicious, relentless, and escalating campaign of assaults against Plaintiffs, including, but not limited to, harassment by telephone and email, online hacking, phishing, identity theft, and other cyberattacks, and even threats of death and bodily harm made toward Tumey and his family.

---

<sup>1</sup> The Voice Tech patents at issue are U.S. Patent Nos. 9,794,348 and 10,491,679 (the “Patents”).

<sup>2</sup> The Patent Suits are *Voice Tech Corporation v. Mycroft AI Inc.*, W.D.Mo. Case No. 4:20-cv-111, and *Mycroft AI Inc. v. Voice Tech Corporation*, W.D.Mo. Case No. 4:20-cv-662.

<sup>3</sup> The IPR Proceedings are *Unified Patents, LLC v. Voice Tech Corporation*, IPR2020-01018, and *Mycroft AI Inc. v. Voice Tech Corporation*, IPR2020-01739.

4. While the aggressors have used highly-sophisticated techniques designed to conceal the source of this information warfare assault, the nature of the attacks, the chronology, and the record of this case compellingly demonstrate that Defendant Mycroft and two of its founders and managing executives: its CEO, Lewis, and its First Officer, Montgomery – self-declared “folks who specialize in information warfare” – are behind them.

5. Indeed, not only have the assaults directly corresponded with events in the Voice Tech Matters—including events that would not have been publicly or widely known—but the Defendants have openly published articles online revealing their role.

6. For instance, a post by Montgomery to Mycroft’s website just as the attacks began depicted Montgomery dressed as a “troll hunter” in chain mail battle armor, with Plaintiffs cast as the ostensive “trolls” he is hunting, and included menacing comments against Plaintiffs such as:

I don’t like letting these matters go quietly. In my experience, it’s better to be aggressive and ‘stab, shoot and hang’ them, then dissolve them in acid. Or simply nuke them from orbit, it is the only way to be sure.

*See Article: Troll Hunter—Mycroft’s Position on Patent Trolls*, published on February 5, 2020, a true and correct printout of which from [Mycroft.ai/blog/troll-hunter-mycrofts-position-on-patent-trolls/](https://mycroft.ai/blog/troll-hunter-mycrofts-position-on-patent-trolls/) (as captured on April 2, 2020) is attached hereto as **Exhibit 1**.

7. This Court already found in one of the pending Patent Suits that, at a minimum, the harassment that Plaintiffs received around the time of this post was at least induced by Montgomery’s post, and ordered Mycroft to remove certain of its content.

8. Yet, the attacks continued and even increased in ferocity, at times virtually shutting down Tumey L.L.P.’s communication systems, and intruding across the boundary into Tumey’s private life as well—including by hacking into personal emails between Tumey, his wife, and their young daughter about the daughter’s school.

9. And, recently, Defendants have even been so bold as to publish new menacing comments on their website, seeming to admit they are the perpetrators of the assaults against Plaintiffs by boastfully taunting that Plaintiffs should not “pick fights with folks who specialize in information warfare. You’ll get your ass kicked.” See Article: *Mycroft Defeats Patent Trolls...Again...For Now*, published on October 15, 2020, a true and correct copy of which from <https://mycroft.ai/blog/mycroft-defeats-patent-trolls-again/> (as captured on October 26, 2020) is attached hereto as **Exhibit 2**.

10. As explained below, this campaign has continued for months and has involved a range of concerted, insidious, and highly injurious assaults.

11. The level of the “information warfare” unleashed by Defendants can hardly be understated. And, as it was intended to do, it has caused and is causing substantial harm to Plaintiffs, including not only monetary damage, but also emotional distress, business interruptions, damage to professional relationships and reputation, and other irreparable injuries.

12. Moreover, Defendants’ reprehensible efforts to chill Plaintiffs’ participation in the proper, judicial resolution of the Voice Tech Matters are an affront to the justice system and to the public as a whole.

13. Although Plaintiffs have taken steps to seek relief from Defendants’ attacks against them, including reporting the conduct described herein to authorities and retaining the services of a cyber-expert to investigate the attacks and defend their systems, these actions have failed to deter Defendants from continuing to engage in an ongoing pattern of abusive and illegal activity against the Plaintiffs.

14. Thus, this suit is filed to enjoin and obtain relief from Defendants’ ongoing aggressive information warfare campaign.

15. In this lawsuit, Plaintiffs assert claims for: (1) violation of the Racketeer Influenced and Corrupt Organization Act (“RICO”) pursuant to 18 U.S.C. § 1962(c); (2) conspiracy to violate RICO pursuant to 18 U.S.C. § 1962(d); (3) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (4) violation of the Stored Wire and Electronic Communications Act (“SCA”), 18 U.S.C. § 2701 *et seq.*; (5) computer tampering in violation of §§ 569.095, RSMo.; (6) Breach of Computer Security in violation of Tex. Civ. Prac. & Rem. Code § 143.001; (7) intrusion on seclusion; (8) tortious interference with business expectancies; (9) assault and battery; and (10) intentional infliction of emotional distress.

16. For all of these reasons, and those set forth further below and as will be shown in this case, Plaintiffs seek immediate and permanent injunctive relief, compensatory and punitive damages, as well as other statutory relief provided for under the Federal Acts asserted, including treble damages, attorney’s fees and costs, and other available relief, as prayed for below.

### **THE PARTIES**

17. Plaintiff Tumey L.L.P. is a Texas limited liability partnership with its principal place of business at 5177 Richmond Avenue, Suite 1188, Houston, Texas 77056. All of Tumey L.L.P.’s partners reside in Texas.

18. Plaintiff Tod T. Tumey is a resident of the state of Texas. Tumey is the managing partner of Tumey L.L.P.

19. Defendant Mycroft AI Inc. is a Delaware corporation with its principal place of business at 300 E. 39th Street, Kansas City, Missouri 64111. Defendant may be served through its registered agent, National Registered Agents, Inc., at 120 South Central Avenue, Clayton, Missouri 63105.

20. Defendant Joshua Montgomery is, upon information and belief, a resident of the state of Hawaii. Montgomery holds himself out as a founder of Mycroft. According to publicly-available information, he was Mycroft's CEO until in or around March of 2020, and has continued on as a managerial executive of Mycroft since that time under the title "First Officer."

21. Defendant Michael Lewis is, on information and belief, a resident of the state of California. Lewis claims to have been among the original financial backers of Mycroft, and has been Mycroft's CEO since in or around March 2020. Upon information and belief, Lewis stands to have a considerable financial gain if the continuous barrage of attacks succeed, and Plaintiffs are thereby unable or unwilling to continue the Patent Suits.

### **JURISDICTION AND VENUE**

22. This Court has federal question jurisdiction pursuant to 28 U.S.C. § 1331 over Counts I - IV of this Complaint, which are claims asserted under the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c) and (d) ("RICO"), the Federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*, and the Stored Wire and Electronic Communications Act ("SCA"), 18 § U.S.C. 2701 *et seq.*

23. This Court has supplemental jurisdiction over Plaintiffs' other claims pursuant to 28 U.S.C. § 1367(a) because the other claims are closely related to Plaintiff's Federal claims, are part of the same case or controversy and derive from a common nucleus of operative facts.

24. This Court also has diversity jurisdiction pursuant to 28 U.S.C. § 1332 over all Counts against Defendants as the parties to this action are citizens of different states, and the amount in controversy exceeds \$75,000 exclusive of interest and costs.

25. This Court has personal jurisdiction over all Defendants. Defendants Montgomery and Lewis regularly conduct business out of Mycroft's principal place of business in this judicial

district. In all actions relevant to this Complaint, Montgomery and Lewis acted as agents of Mycroft and/or acted out of their own personal interest and financial stake in that company. Defendant Mycroft maintains its principal place of business in this judicial district and regularly conducts business in this judicial district.

26. Defendants all have continuous and systematic contacts with this judicial district. They have purposefully availed themselves of the privilege of conducting activities in this judicial district and have enduring contacts in this District.

27. Defendants are subject to personal jurisdiction in this judicial district through their regular transaction of business in this state and their commission of tortious acts within the state. § 506.500, R.S. Mo.

28. Based on information and belief, venue is proper in this District pursuant to 28 U.S.C. §§ 1391, as Defendant Mycroft maintains its principal place of business in this judicial district and as it is the judicial district in which a substantial part of the events or omissions giving rise to this action occurred. Venue is also proper under 18 U.S.C. § 1965(a) as one or more Defendants reside and/or transact their affairs within this District.

### **FACTS**

#### **A. Defendants' Interrelationships and "Information Warfare" Background**

29. Mycroft is a technology business that claims to provide "the world's leading open source voice assistant."

30. As noted, Montgomery is a founder and former CEO of Mycroft, and currently serves as Mycroft's "First Officer."

31. According to Mycroft's website, Montgomery is "a hacker at heart." *See* <https://mycroft.ai/media/#leadership> (last accessed January 13, 2021), screen capture attached hereto as **Exhibit 3**.

32. And, Montgomery has also publicly self-identified as a “hacker.” *See* Montgomery’s Profile on Medium.com, <https://medium.com/@joshuamontgomery/about>, attached hereto as **Exhibit 4**; *see also* <https://www.linkedin.com/in/joshuawmontgomery> (last accessed February 18, 2021) (claiming to be a “Certified Ethical Hacker”), screen capture attached here to as **Exhibit 5**.

33. In addition, Montgomery’s introductory post as Mycroft’s CEO to the online Mycroft Community Forum in or around September 2015 touts his background as an “Information Warfare Officer” for the military. *See* <https://community.mycroft.ai/t/bulb-introduction-joshua-montgomery-ceo-of-mycroft-a-i/104> (last accessed February 18, 2021), screen capture attached hereto as **Exhibit 6**.

34. Michael Lewis is the current CEO of Mycroft.

35. According to Lewis and Mycroft’s published statements, Lewis is one of Mycroft’s original and largest investors, and he has been effectively “bankrolling” Mycroft’s operations for at least the last year.

36. Lewis has publicly stated that he and Montgomery are a team who manage and run Mycroft together.

37. Lewis, like Montgomery, also has a background in sophisticated computer techniques and software.

38. Upon information and belief, Defendants’ particular skill, expertise, and resources uniquely position them to be able to execute the sophisticated information warfare unleashed against the Plaintiffs here.

39. And upon further information and belief, they have been doing so.



**B. Plaintiffs' Initial Outreach to Defendants in the Course of Their Representation of Voice Tech**

40. As referenced, Plaintiffs are counsel for Voice Tech, the owner of two Patents issued by the United States Patent and Trademark Office, which Voice Tech contends Mycroft has infringed.

41. On November 11, 2019, Plaintiff Tod Tumey, as counsel for Voice Tech, began sending correspondence to Montgomery, then Mycroft's CEO, in an effort to address Mycroft's alleged infringement without resorting to litigation.

42. Tumey's letters and emails to Mycroft advised it of Voice Tech's patents in the same field as Mycroft's products, offered terms for a license to resolve the dispute, and invited Mycroft to contact him to discuss the matter.

43. Chris DeBacker, an attorney, eventually contacted Tumey in response to his correspondence to Mycroft, but informed Tumey that he was unsure yet whether Mycroft was engaging him in relation to this matter and did not have a response from Mycroft to Tumey's overture.

44. Even after DeBacker was retained by Mycroft, neither he nor Mycroft provided any substantive response to Voice Tech's overtures.

45. Having tried for two months without success to engage Mycroft in discussions about Voice Tech's Patents, Tumey L.L.P. filed a patent infringement complaint in the Eastern District of Texas on January 9, 2020.

46. Tumey was not counsel of record in the suit filed in the Eastern District of Texas. Rather, the public filings in that case listed Eric Adams, another attorney with Tumey L.L.P., as the lead (and only) counsel of record for the firm in that suit.

47. Behind the scenes, though, Tumey remained the point person in Tumey L.L.P.’s communications with Mycroft and Mr. DeBacker, who Mycroft did retain as its counsel.

48. Thus, on January 9, 2020, when the case was filed, Tumey sent a courtesy copy of the complaint to Mr. DeBacker and again invited licensing discussions.

49. Thereafter, on January 23, 2020, Tumey sent Mr. DeBacker proposed terms for a resolution. Mr. DeBacker acknowledged receipt of the licensing proposal on the same day.

50. But, by January 31, 2020, Mycroft and Mr. DeBacker still had not provided any substantive response.

51. Accordingly, that day, Friday, January 31, 2020, Tumey L.L.P. served Voice Tech’s Eastern District of Texas Complaint on Mycroft.

### **C. Defendants’ Threats and Illegal Conduct Begins**

#### **1. The First Wave of Attacks**

52. Almost immediately after serving Mycroft with the lawsuit on January 31, 2020—by Monday, February 3, 2020—Voice Tech’s law firm, Plaintiff Tumey L.L.P., began receiving repeated harassing phone calls in which someone would call its office and breathe heavily before hanging up.

53. Neither these type of phone calls nor the rest of the information warfare campaign that followed, as described below, were a normal occurrence for Plaintiffs.

54. Two days after the calls began, on February 5, 2020, Mycroft published an article on its website, written by its then-CEO, Joshua Montgomery, entitled “Troll Hunter—Mycroft’s Position on Patent Trolls.” The post included threats of physical harm and death against Plaintiff Tumey. Specifically, the post argued that, in dealing with counsel like Voice Tech’s, “it’s better to be aggressive and ‘stab, shoot and hang’ them then dissolve them in acid.” And, it urged others to share and repost Montgomery’s vitriolic assault. *See* Article, attached hereto as **Exhibit 1**.

55. The next day, on February 6, 2020, Defendants also republished the article from February 5, 2020 advocating for Tumey’s grisly death and posthumous corpse desecration onto Mycroft’s Facebook® page as “[a]n important message from our CEO;” as well as to Mycroft’s Twitter® account, and Reddit®. **Exhibit 7 at TUMEY000001-8.**

56. Then, just after midnight following Defendants’ online activities, Plaintiffs began receiving a series of hostile and harassing emails to both Tumey L.L.P.’s general email account and Tumey’s individual account, from seemingly fictitious accounts set up for this purpose. True and correct copies of these and other emails received by Plaintiffs that are believed to be part of the Defendants’ information warfare campaign against them are attached hereto as **Exhibit 7** (“Cyberattack Chronology”).

57. Although the emails were ostensibly presented anonymously, they repeated and were reminiscent of the language, level of vitriol, and other characteristics of Montgomery’s blog. By way of illustration, as Montgomery had done in his posted article, the emails graphically recommended grisly and highly disturbing death and acts of violence against Tumey. *See, e.g., Exhibit 7 at TUMEY000010* (February 7, 2020 10:11 a.m. email to Tumey L.L.P. (“...then drown yourself with a red hot iron rod shoved up your ass.”). And, referred to Tumey as a “patent troll,” just as Montgomery had done online. *See Exhibit 7 at TUMEY000011.* (February 7, 2020 11:31 a.m. email to Tumey (“Patent troll go back under your scummy bridge.”)).

58. On February 8, 2020, Mycroft republished the article from February 5, 2020 on Hacker News Digest. **Exhibit 7 at TUMEY000012-16.**

59. Later in the day on February 8, 2020, Plaintiff Tod Tumey began receiving notifications of efforts to change passwords and of a hack attempt into his personal Facebook®

account, and another alert that an attempt had been made to create a Twitter® account using his name. **Exhibit 7 at TUMEY000021.**

60. Mere minutes later, on February 8, 2020, someone using Tumey's personal information began to sign him up for various online memberships, mailing lists, inquiries about debt relief services, and insurance quotes, among other things. **Exhibit 7 at TUMEY000017-20, 23-94.**

61. One such insurance quote ominously asked for information related to one of Tumey's family vehicles, an Audi. This inquiry was followed up immediately with an email to the Tumey L.L.P. general email account stating "Nice Audi." **Exhibit 7 at TUMEY000037.**

62. Plaintiff Tumey L.L.P. law firm then received multiple notifications from GoDaddy® that unauthorized attempts had been made to access (and presumably tamper with) the Tumey L.L.P. website account and emails, and to change associated passwords. **Exhibit 7 at TUMEY000039-40.**

63. These unauthorized access attempts to the Tumey L.L.P. firm system were followed up with emails indicating that someone was using Tumey's personal information to sign him up for various pornography websites and numerous other mailing lists. **Exhibit 7 at TUMEY000047-49.**

64. The next day, on February 9, 2020, an email address was created by someone using Tumey's name ([TodTumey@gmx.com](mailto:TodTumey@gmx.com)) and was used to send a very disturbing, violence-filled email to Tumey, which included horrific comments about Tumey's children. **Exhibit 7 at TUMEY000095-97.**

65. The timing and pattern of these activities, as well as the nature of the emails, and similarities and connections with Montgomery's published posts led Plaintiffs to conclude that

Montgomery and Lewis, alone or acting in concert with others, were most likely the individuals behind this onslaught of harassment.

66. Fearful of Defendants' vitriolic assaults and seeming lack of limits, Tumey notified the police, increased security at his home for the protection of his family, and similarly increased security precautions at Tumey L.L.P., including locking the firm's doors at all times, bolstering its online security systems, and alerting its building security and property management.

67. In the wake of this abuse, and in an effort to further protect Tumey, his family, and his firm from potential risk, on February 11, 2020, Voice Tech voluntarily dismissed the infringement lawsuit in Texas with a view towards refileing it in Missouri (*i.e.*, in Mycroft's home state and away from Tumey's residence and business) in hopes that it might temper Mycroft's bad faith conduct, avoid any disputes over venue, and more efficiently allow the litigation to proceed on the merits.

68. Defendant Montgomery, in response, purported to claim victory by virtue of the voluntary dismissal, and—consistent with the fact that Defendants had been behind the flurry of assaultive behavior—the “anonymous” emails and online harassment all abruptly stopped. *See* Article “Patent Troll Update”, dated 2/19/2020, attached here to as **Exhibit 8**.

## **2. The Second Wave of Attacks**

69. Voice Tech refiled the patent infringement lawsuit in the Western District of Missouri with Tumey L.L.P. as its counsel of record in the case.

70. Given Plaintiffs' experience after the case was filed in Texas, on April 2, 2020, Voice Tech filed a Motion for Relief to Require Decorous and Civil Conduct by the Parties in the Western District of Missouri, seeking intervention by the Court related to the cyberattack harassment activity and threatening, inflammatory posts that had occurred.

71. Almost immediately after the Motion for Relief was filed by Voice Tech, the cyberattacks toward Plaintiffs and Tumey's family resumed.

72. On April 5, 2020, unauthorized attempts were again made to remotely access Tumey L.L.P.'s servers.

73. Also on April 5, 2020, Tumey's wife had her Twitter<sup>®</sup> account suspended due to too many access attempts.

74. On April 6, 2020, Plaintiff Tumey L.L.P. began receiving phone calls from companies responding to online requests for information they had reported having received over the weekend (April 3-5, 2020).

75. On April 14, 2020, a remote hearing was held on Voice Tech's Motion for Relief and the Court granted Voice Tech's Motion. The Court found that, whether or not Montgomery had personally perpetrated the conduct at issue, there was, at a minimum, "sufficient evidence that the harassment that plaintiff's counsel has received is induced or inspired by the postings of Mr. Montgomery." *See* Case No. 4:2020-cv-111, Doc. No. 23, Hearing Transcript dated April 14, 2020, at 13:22-24. The Court further ordered that certain portions of the online posting by Mycroft be removed. *Id.*

76. While a minute entry notation was made on the Court's docket after the hearing concluded on April 14, 2020, the entry noted only that a hearing was held and a "ruling" was made; it did not note what the ruling was. [Case No. 4:2020-cv-111, Docs. 22-23]. Further, the transcript of the hearing was not released to the public until July 20, 2020. [Case No. 4:2020-cv-111, Doc. 23].

77. Nevertheless, almost immediately after the Court granted Voice Tech's Motion for Relief, the cyberattacks experienced by Plaintiffs again intensified.

78. On April 16, 2020, less than 48 hours after the hearing concluded (and before the Court's ruling was publicly available), Plaintiff Tumey received a phishing message purporting to be an email notifying Tumey that he had a voicemail and that he should click on the provided link to listen to it. This phishing email was a targeted attack on the Tumey L.L.P. firm. The email's embedded link was a sophisticated virus designed to evaluate the type of cyber defenses the Tumey L.L.P. firm had in place and to obtain the username and password for the Firm's GoDaddy® account. **Exhibit 7 at TUMEY0000108.**

79. The cyberattacks continued thereafter, including that on April 27, 2020 a voluminous batch of fake emails were sent out from Plaintiff Tumey L.L.P.'s email domain under the name of a fictitious attorney of the firm, Sarah Millican, regarding an alleged wire transfer confirmation. These fake emails were sent to hundreds (if not thousands) of law firms and other businesses both inside and outside of the United States. **Exhibit 7 at TUMEY000109-147.**

80. Upon information and belief, the distribution list for the fake email was intentionally designed to target persons and entities that were likely to be Plaintiffs' clients and potential clients, and others with whom Plaintiffs was likely to have existing or potential business relationships.

81. This round of fake emails caused Plaintiffs to be inundated with a deluge of response emails and/or bounce-back, delivery failure email messages, as well as phone calls from recipients of the cyberattack emails such that, for significant periods of time, it was impossible to send out any emails or make or receive any phone calls at the Tumey L.L.P. law firm.

82. These attacks continued for days and forced Plaintiffs to hire a computer specialist to assist with crafting a defense.

83. The specialist eventually determined that the attacks emanated from two servers in Japan. After Plaintiffs' computer specialist contacted the server company in Japan, the servers were closed down and the attacks ceased on May 1, 2020.

84. The assault subsided for roughly a week, until the parties exchanged their initial disclosures on May 6, 2020.

85. Although those disclosures were traded privately and not filed, another wave of targeted attacks against Plaintiffs began after they were served.

86. This massive wave of attacks again sent out a vast amount of fake spam emails, purportedly on behalf of Tumey L.L.P., to law firms and business all over the world. **Exhibit 7 at TUMEY000818-853.**

87. The Plaintiffs' computer specialist identified that this round of attacks was being routed from a server in Vietnam (utilizing a nearly identical set-up as the first round of attacks that routed from servers in Japan), and that server was shut down after the computer specialist contacted the Vietnamese server company.

88. Even after the servers routing the cyberattacks were shut down, Plaintiffs continued to experience significant impacts on the firm's email accounts as a result of the attacks (e.g., firm email accounts were designated internationally as spam providers) that rendered business communication nearly impossible for a period of time.

89. Thus, just a few weeks after the Court's order on Voice Tech's Motion for Relief, Plaintiffs were the victim of two large cyberattacks that hindered its ability to serve its clients, forced it to incur significant expenses in lost time and productivity, as well the cost of engaging a computer specialist to assist in defending against the attacks.



90. Part of Plaintiffs' business includes working with foreign attorneys needing United States local counsel to handle intellectual property matters here in the United States. In addition, Plaintiffs routinely work with attorneys from all over the United States on various intellectual property matters.

91. These cyberattacks not only virtually shut down operations of the Tumey L.L.P. law firm for days, but severely injured the reputation of Plaintiffs with future business contacts all over the United States and in other countries.

92. Upon information and belief, Plaintiffs lost clients and future business as a result of these attacks.

93. Upon information and belief, the fake email distribution was also designed to damage and did damage Plaintiffs' reputation, relationships and/or opportunities to have future relationships with the recipients.

94. Upon information and belief, these injuries and losses were intended results of the mass fake-email distributions, which were designed to cripple Plaintiffs' communication systems and cast its business and attorneys in an unfavorable light.

95. After these two sophisticated cyberattacks against the Tumey L.L.P. law firm, Plaintiffs took additional cybersecurity measures to deter and detect future attacks at its expense.

### **3. The Third Wave of Attacks and the Targeting of Tumey's Minor Daughter**

96. On May 27, 2020, Voice Tech served Mycroft with its infringement contentions. This was, again, not a publicly-available document.

97. Less than 24 hours later, several additional cyberattacks on Plaintiffs occurred.

98. First, the firm's computer specialist detected a spike in attempts to hack into the firm's website.

99. Second, on May 28, 2020, Plaintiffs received a phishing email allegedly from GoDaddy® in yet another attempt to gain access to Plaintiffs' computer systems. **Exhibit 7 at TUMEY000926.**

100. On May 29, 2020, Voice Tech served its First Set of Interrogatories on Mycroft, another document that was not filed publicly.

101. Within days, on June 1, 2020, Plaintiffs' protected computers, computer systems and facilities through which its electronic communication service is stored, were accessed without authorization and one or more Tumey L.L.P. email accounts were improperly accessed.

102. Specifically, an email exchange between Tumey, his wife, and their 12-year old daughter about an email from the daughter's school was improperly accessed and reviewed on the system. The hacker then used the daughter's account to reply to her father, Tumey, from the misappropriated email, asking that he click on a link to fill out a permission form. **Exhibit 7 at TUMEY000934-936.**

103. The link embedded in this fake phishing email contained an ultra-sophisticated virus designed to improperly access Plaintiffs protected computer systems.

104. The same day, June 1, 2020, the firm's computer specialist again detected a spike in attempts to hack into the firm's system.

#### **4. Attacks Continue**

105. Plaintiffs have continued to experience ongoing cyberattacks and hacking attempts against the firm and its personnel (including but not limited to harassing phone calls, phishing scam emails, and hacking attempts on personal and business accounts, including hacking attempts on the firm's system), with such attempts intensifying after events—including non-public events—in the Patent Suits.

106. For example, on June 12, 2020, Mycroft approached Voice Tech about pushing off a mediation scheduled for July 6, 2020. When Voice Tech would not agree to delay the scheduled mediation, Plaintiffs immediately received an onslaught of harassing phone calls, phishing scam emails, and increased hacking attempts on their system.

107. On July 20, 2020, Voice Tech emailed a letter to Mycroft regarding noncompliance with the Court's April 14, 2020 order requiring Mycroft to remove certain published statements posted online. That same day, and in the days immediately following such letter, Plaintiffs received multiple phishing emails.

108. In early December 2020, after a number of events occurred in the Voice Tech Matters, including the parties' submission of non-public mediation materials in preparation for a mediation with the MAP director, Tumey's eldest daughter received notifications from Facebook on December 8, 2020 that her account had been temporarily locked due to recent, unfamiliar login attempts. **Exhibit 7 at TUMEY000968.**

109. On December 16, 2020, counsel for Voice Tech privately informed Mycroft's counsel that the cyberattacks and harassment experienced by Plaintiffs was continuing, and that Plaintiffs had hired a computer specialist who was looking into these activities.

110. Voice Tech's counsel mentioned to Mycroft's attorney that the bio of the new computer specialist may be posted on the Tumey L.L.P. firm's website, but did not mention the person's name.

111. To test their theory that sharing this information might prompt another attack, Plaintiffs had previously posted a shell profile for their specialist on the Tumey L.L.P. firm's website under the pseudonym "Paul Weller." The shell profile for Paul Weller on the firm's website also included a link to a shell professional website for Paul Weller. Both the shell profile

for Paul Weller on the Tumey L.L.P. firm website and the shell professional website of Paul Weller were first published just a few hours before noting the existence of “Paul Weller” to Mycroft’s attorney.

112. Within hours of telling Mycroft’s counsel about the specialist on December 16, 2020, an attempted hack was detected on “Paul Weller’s” shell professional website (a link to this website was provided in Paul Weller’s bio on the Tumey L.L.P. firm site). Over the next 24 hours, several hacks and exploits were detected. Paul Weller’s professional website was not publicly linked from any search engine during this time (indicating that it was being accessed only through the link provided on the Tumey L.L.P firm site). From the time the Paul Weller website went live, until when Google<sup>®</sup> first indexed the website, five different hack attempts were detected.

113. Since the shell professional website for Paul Weller went “live” on December 16, 2020, it has continued to be the target of ongoing and sophisticated cyberattacks.

114. A chronology summarizing and further detailing cyberattacks and other forms of information warfare experienced by Plaintiffs along with events in the Voice Tech Matters that coincided with and are believed to have precipitated them, as discussed above, is attached hereto as **Exhibit 7** (“Cyberattack Chronology”).<sup>4</sup>

115. The aforescribed assaults against Plaintiffs are likely not exhaustive of the full campaign of information warfare employed against them. Rather they are illustrative of such attacks, as Plaintiffs have been able to identify and detect them.

---

<sup>4</sup> The Cyberattack Chronology at Exhibit 7 is a non-exhaustive summary of the attacks; attacks are ongoing and the record is simply too voluminous to include in the chronology in its entirety.

**D. The Evidence Points to Defendants as Perpetrators**

116. Upon information and belief, the cyberattacks described in the paragraphs above, and further detailed in **Exhibit 7**, were committed by or at the direction of the Defendants and/or were purposely incited by them.

117. While such sophisticated cyberattacks by design conceal their true source, the circumstances of this case, including the timing and targeted nature of the attacks, and the public proclamations by Defendants regarding their hacking experience and expertise in “information warfare,”—including directly in reference to the Voice Tech Matters—reveal that Defendants are the source of the attacks.

118. In an online article written by Montgomery and published on Mycroft’s website, Defendants give their own summary of events in the case between Voice Tech and Mycroft and explains what is going to happen to Voice Tech:

Will bankrupting and demolishing their professional reputation be enough? Maybe. But if Voice Tech is simply a façade under which a group of unscrupulous attorneys are trying to extort money from honest actors, we will “[pierce the corporate veil](#)” and come after the principal’s homes, cars, savings, and other assets.

*See* “Mycroft Defeats Patent Trolls...Again...For Now” at 4, attached hereto as **Exhibit 2**.

119. At the end of the article, under a section entitled “The Moral of the Story,” Defendants say “don’t pick a fight with a pair of founders who’s prior reputation was built on beating the telecommunications lobby, and fighting off bullshit assertions from Marvel” – on information and belief, referring to Montgomery and Lewis as the “pair of founders” by reference to their past exploits. And, in the very next sentences, issue a dire warning about the consequences

of doing so: “Finally, don’t pick fights with folks who [specialize in information warfare](#). You’ll get your ass kicked.”<sup>5</sup>

120. That last part of the warning in blue lettering is a link to a news article entitled “Red Cell Challenges Cyber Warriors in Multiforce Exercise,” written in April 2017 for a U.S. Defense Department publication. *See* **Exhibit 9**.

121. The news article starts off by stating, “Air Force Capt. Joshua Montgomery isn’t a criminal, but he plays one as part of his duties.” *Id.* at 1.

122. It goes on to explain that “Red Cell members, such as Montgomery, play the role of adversary hackers.” *Id.* at 3. In this same article, Montgomery is quoted as saying:

“It’s the best job in the military,” he said. “We get to break things. We get to go and do all the things that would send you to jail in the real world. It’s fantastic.”

...

“The idea of an information aggressor squadron is to understand the tactics that real-world adversaries like hackers and corporate espionage agents use,” he explained.

123. Taken together, the article “Mycroft Defeats Patent Trolls...Again...For Now” and the article, “Red Cell Challenges Cyber Warriors in Multiforce Exercise,” as linked therein, read as an implied, if not express, admission that Mycroft, Montgomery, and Lewis have used and will continue to use information warfare tactics against Plaintiffs and others who would seek to pursue claims and enforce rights against them.

---

<sup>5</sup> *See* Dr. Waseem Ahmad Qureshi, [Information Warfare, International Law, and the Changing Battlefield](#), 43 Fordham Int’l L.J. 901, 907–08 (2020) (noting that the U.S. Air Force defines “information warfare” as “any action to deny, exploit, corrupt, or destroy the enemy’s information and its functions” and that “cyberwarfare” is one dimension of information warfare which relies on the internet and computers through “viruses, hacking, and malware attacks on an adversary’s strategically important computer systems”).

124. Further, as demonstrated by the allegations above and the timeline of events, there is an unquestionable link between activity in the Voice Tech Matters and the cyberattacks experienced by Plaintiffs.

125. Whenever something happened in the Voice Tech Matters that Defendants did not like or found to be unfavorable (like when the Court granted Voice Tech's Motion for Relief), the cyberattacks increased. When something happened in Defendants' favor (like the voluntary dismissal of the patent infringement action filed in Texas), the attacks slowed down or ceased all together.

126. Further, many events in the Patent Suits that triggered targeted cyberattacks on Plaintiffs, like the Court's ruling on the Motion for Relief, were not made public or known to anyone but the parties (on the Motion for Relief, the Court's ruling was not made public until months later, when the transcript of the hearing was made public).

127. The cyberattacks experienced by Plaintiffs were of a very sophisticated nature, targeted and designed to avoid detection. The viruses and hacking techniques utilized were not "off-the-shelf" attacks frequently utilized in the average hacking or phishing schemes. Instead, these were targeted attacks crafted by someone experienced in "information warfare" and with the skill to cover their tracks.

#### **E. The Mycroft Enterprise**

128. The unlawful activities described above and perpetrated by the Defendants occurred in connection with the operation of Mycroft, an incorporated business that affects interstate commerce. Defendants Montgomery and Lewis intentionally and knowingly misused their control over Mycroft, an otherwise legitimate business entity, to undertake and perpetrate these illegal acts against Plaintiffs.

129. This enterprise will hereinafter be referred to as "the Mycroft Enterprise."

130. The participants in the Mycroft Enterprise advocate for a supposed mission of promoting “open source innovation;” *i.e.*, the creation of new inventions which are then handed over by the inventor for free use by others.

131. In reality, this is not an altruistic mission for the Mycroft Enterprise participants. To the contrary, they stand to and do gain directly from this so-called “mission” in multiple ways.

132. For instance, the Mycroft Enterprise gains directly from inventors who are swayed by them to give over their innovations to the so-called open source movement. In particular, the Mycroft Enterprise can then use—and financially profit from—the “open source innovations” contributed by others without any compensation to the inventor. By so doing, the Mycroft Enterprise reaps all of the benefits of the inventor’s hard work and inspiration.

133. The Mycroft Enterprise also stands to and does benefit from its promotion of open source by allowing certain of its own innovations to be used as open source thereby creating its own market for the products it sells that incorporate its own open source contributions.

134. In short, upon information and belief, the Mycroft Enterprise’s business model is built and predicated upon the promotion of its open source mission for its own gain. As such, inventors who do not freely hand over their patented innovations for Mycroft, like Voice Tech, and the attorneys who would seek to protect and enforce those patent rights for them, like Plaintiffs, are a threat to the Mycroft Enterprise’s business interests.

135. Indeed, the Mycroft Enterprise participants publicly and frequently express their disdain for and anger towards such entities and people.

136. Thus, in undertaking their abusive conduct toward Plaintiffs, Defendants Montgomery and Lewis, as members of the Mycroft Enterprise, had a common purpose: to punish the proper assertion of patent infringement rights (including the obstruction of any counsel who



would represent clients in the prosecution of such intellectual property rights) in order to advance their own pecuniary and business interests, and to ultimately gain an undue advantage in the pending Voice Tech Matters.

137. Upon information and belief, Defendants Montgomery and Lewis, and those acting in concert with them or at their direction, in furtherance of this common goal, undertook to gain an undue advantage in the pending Voice Tech Matters through illegal harassment, threats and damage to the Tumey L.L.P. law firm and its attorneys, such that they would be unable or unwilling to continue prosecuting the Voice Tech Matters filed against Mycroft by Tumey L.L.P. on behalf of its client.

138. Mycroft's business model is based on the promotion of an open source sharing of technology (not charging for the use of the software but for the tooling and platform to consume the software as a service, via a subscription); and as a result, as part of this promotion of open-source community, Mycroft wishes to utilize and profit from the innovation and patented technology of others for free.

139. Voice Tech dedicated over a decade to prosecuting its patents through the USPTO in order to obtain them. As a matter of public policy, in order to incentivize innovation, our legal system grants such intellectual property rights and protects them.

140. Because Voice Tech's assertion of its lawfully obtained intellectual property rights is in direct conflict with Mycroft's open-source business model for success, Voice Tech's assertion of its rights is something that the Mycroft Enterprise has undertaken to punish through targeted and sophisticated ongoing cyberattacks against the Plaintiffs, as counsel for Voice Tech.

141. The Defendants Montgomery and Lewis held executive, managerial roles at Mycroft and exercised a managerial role in the Mycroft Enterprise's affairs.

142. The cyberattack activities undertaken by Defendants constitute “racketeering activity” as defined in 18 U.S.C. § 1961. Specifically, as outlined below in Count I, the Defendants’ conduct, as described in detail in the paragraphs above, are crimes perpetrated against Plaintiffs and are violations of the wire fraud act, are tampering with and retaliation against witness crimes, and constitute internet threats, all in violation of federal law.

143. Defendants’ pattern of racketeering activities over the last year constitutes an open-ended scheme that poses a threat of continuity in that the conduct by its very nature projects into the future with a threat of repetition.

144. As discussed above, the goal of the enterprise is to further the business success of Mycroft by eliminating (through any means), any potential assertion of patent infringement rights that threatens Mycroft’s promotion of its “open source” mission.

145. Moreover, the Voice Tech Matters that have motivated Defendants’ attacks are still in relatively early stages, and may well continue for years. Indeed, the Patent Suits are currently stayed pending resolution of the IPR Proceedings.

146. Thus, there is every indication that, absent intervention, Plaintiffs will continue to experience ongoing cyberattacks and harassment at the hands of Defendants, with such attacks intensifying anytime something happens in the Voice Tech Matters that the Defendants do not like. The conduct undertaken by the Defendants over the past 12 months, as described herein, shows that there is no limit to the lines Defendants will cross, or the “information warfare” tactics they will employ, to further their goal of eliminating perceived threats to the ultimate success of Mycroft.

147. In addition, the public statements made by Defendants on behalf of Mycroft show that this practice of intimidation and threats to use “information warfare” against its opponents,

including their cyberattack and hacking expertise, is part of the Mycroft Enterprise's regular way of doing business.

148. By reason and as a result of Defendants' conduct and participation in the conduct alleged herein, including the racketeering activity in violation of 18 U.S.C. § 1962, they have caused damages to Plaintiffs in their business and property.

149. This damage includes, but it is not limited to, actual financial loss in the form of employee time spent addressing and responding to hacking attacks, hiring a computer specialist to defend against such attacks, costs associated with increased security (both physical and virtual) at Plaintiffs' offices and home, the inability to access Plaintiffs' property (firm phone lines and email accounts) for the significant periods of time when functionality was entirely shut down due to the volume of cyberattacks, and business loss damage in the form of reputational injury, lost clients, and loss of potential business and business expectancy.

150. In addition, Defendants' actions employed force, threats of force, fear and/or violence in an attempt to deprive Plaintiffs of their property interest in running their business and continuing to represent and litigate on behalf of their clients.

151. Finally, the extreme emotional distress inflicted on Plaintiff Tumey through Defendants' onslaught of cyberattacks and threats, both directed at him personally, and at his family, business and livelihood, has been significant.

**COUNT I**  
**Violation of RICO, 18 U.S.C. § 1962(c)**  
**(All Plaintiffs Against Defendants Montgomery and Lewis)**

152. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

153. Defendants' conduct violates the Racketeer Influenced and Corrupt Organization Act ("RICO") pursuant to 18 U.S.C. § 1962(c).

154. The RICO enterprise which was engaged in and the activities of which affected interstate and foreign commerce, is the entity Mycroft (described throughout this Complaint as the "Mycroft Enterprise").

155. Upon information and belief, at all relevant times, Montgomery and Lewis were employed by and/or associated with the illegal Mycroft Enterprise.

156. The Mycroft Enterprise is a legal entity with an organizational structure separate and distinct from the Defendants.

157. Upon information and belief, Montgomery and Lewis agreed to and did conduct and participate in the conduct of the Mycroft Enterprise's affairs, through a pattern of racketeering activity and for the unlawful purpose of intentionally defrauding Plaintiffs.

158. Specifically, upon information and belief, pursuant to and in furtherance of their fraudulent scheme, Defendants engaged in multiple related acts of interstate mail and wire fraud, tampering with and retaliating against witnesses in official proceedings, and numerous and repeated internet threats, all in violation of 18 U.S.C. § 1962(c).

159. The acts of wire fraud, tampering and retaliating against witnesses, and internet threats constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).

160. As described above, the members of the Mycroft Enterprise had a common purpose: to punish the proper assertion of patent infringement rights (including the obstruction of any counsel who would represent clients in the prosecution of such intellectual property rights) in order to promote Mycroft's mission of promoting open source innovation, which is part of Mycroft's

business model for success, and to ultimately gain an undue advantage in the pending Voice Tech Matters.

161. Upon information and belief, the Mycroft Enterprise engaged in tortious conduct that crossed state and international lines, spanning from Texas to Missouri, and utilizing servers and resources from overseas to advance their illegal computer warfare scheme. Upon information and belief, Defendants used their experience and background in advanced and sophisticated hacking techniques to advance the Mycroft Enterprise.

162. Defendants Montgomery and Lewis were both employed by and/or associated with Mycroft during the period in question. Upon information and belief, Montgomery and Lewis conducted the affairs of the Mycroft Enterprise through the pattern of racketeering activity alleged herein.

163. The actions taken by Defendants to advance and serve the Mycroft Enterprise were separate and distinct from any legitimate work Defendants performed for Mycroft.

164. The Mycroft Enterprise has functioned for at least the last 11 months, continues to function as a continuing unit, and maintains an ascertainable structure separate and distinct from the pattern of racketeering activity.

165. The allegations detailed above show that the offenses of the Mycroft Enterprise are part of Mycroft's ongoing regular way of doing business.

166. Defendants themselves have published statements touting their "information warfare" experience as a company mantra for Mycroft and warning others not to cross them.

167. The pattern of racketeering acts spans more than a year. In addition, that pattern of activity poses a threat of continued illicit and illegal activity because it likely will continue indefinitely, or until the currently pending Voice Tech Matters are resolved (which could easily

take years). The racketeering acts discussed herein are all related to each other because they all involve the same targeted victims (Plaintiffs Tod Tumey and his law firm, Tumey L.L.P.) and were designed to advance Mycroft's ultimate goals of business success through its open-source model, by eliminating and punishing any assertions of intellectual property rights that are in conflict with that business model.

168. Plaintiffs hereby allege and set forth the following predicate racketeering activities as defined under 18 U.S.C. § 1961:

**A. RICO Predicate Act #1: Wire Fraud, 18 U.S.C. § 1343**

169. Upon information and belief, Montgomery and Lewis conducted and participated in the affairs of this RICO enterprise through a pattern of racketeering activity that has occurred over the course of many months and continues to this day, and that consisted of numerous and repeated violations of the federal wire fraud statute, which prohibits the use of any interstate or foreign wire or mail facility for the purpose of executing a scheme to defraud, in violation of 18 U.S.C. § 1343.

170. Upon information and belief, Montgomery and Lewis engaged in the formation of a scheme to defraud Plaintiffs in order to illegally gain access to their protected computers and protected computer networks. Such illegal access would provide further ammunition for Montgomery and Lewis in their ultimate goal to wage computer warfare against Plaintiffs in an effort to force Plaintiffs to dismiss or abandon the pending patent infringement lawsuits asserted against Mycroft.

171. For example, upon information and belief, Montgomery and Lewis intentionally conspired to commit numerous acts of wire fraud by obtaining access to Plaintiffs' protected computer network through a scheme or artifice – i.e., through fake phishing emails.

172. As part of and in furtherance of the scheme to defraud, upon information and belief, Montgomery and Lewis made use of the United States wires and made material omissions and misrepresentations to Plaintiffs with the intent to defraud and deceive Plaintiffs.

173. Specifically, in furtherance of the scheme to defraud, upon information and belief, Montgomery and Lewis, sent, mailed, and transmitted, or caused to be sent, mailed, or transmitted, in interstate or foreign commerce, numerous materials, including but not limited to:

a. A fraudulent email sent to Plaintiff Tumey on June 1, 2020. The fraudulent email was disguised by Defendants and made to appear that it was sent from Tumey's daughter's Tumey L.L.P. email account. In the substance of the email Tumey's daughter purported to request that a permission form be filled out for her school, with the goal of tricking Tumey into clicking the link. If Tumey had clicked on the link embedded in the email, it would have given Defendants access to Plaintiffs' protected computers and information.

b. In addition, upon information and belief, on two separate occasions, Defendants sent or caused to be sent, a wave of fake SPAM emails to potential clients and potential business contacts across the world, fraudulently crafted to appear they came from the Tumey L.L.P. law firm. *See Exhibit 7*, attached hereto, which provides a non-exhaustive chronology of these emails. These fraudulent SPAM emails were intended to defraud potential clients and potential business contacts into believing Plaintiffs had sent the unprofessional emails, and cause Plaintiffs to lose current and future business as a result.

174. Upon information and belief, Defendants intentionally mailed or transmitted, or caused to be mailed or transmitted, numerous phishing emails like those described above, making material misstatements therein, with the goal of inducing the targeted individuals at Tumey L.L.P.

law firm to surrender login credentials or click on a link that would give Defendants Montgomery and Lewis access to the Tumey L.L.P. firm's protected systems.

175. Upon information and belief, Defendants Montgomery and Lewis launched the fake email phishing attempts with the specific intent of deceiving and defrauding Plaintiffs so that Defendants could access Plaintiff's protected computers and protected computer networks and advance the Mycroft Enterprise's open-source business model goal through further disrupting, harassing and threatening Plaintiffs to drop the pending lawsuits against Mycroft.

176. Upon information and belief, Defendants Montgomery and Lewis launched the fake SPAM emails to potential Tumey L.L.P. clients with the specific intent of deceiving and defrauding Plaintiffs' potential clients and potential business contacts, causing Plaintiffs to lose current and future business and advance the Mycroft Enterprise's open-source business model goal through further disrupting, harassing and threatening Plaintiffs to drop the pending lawsuits against Mycroft.

177. By reason and as a result of Montgomery's and Lewis' conduct and participation in the racketeering activity alleged herein, they have caused damage to Plaintiffs.

**B. RICO Predicate Offenses #2 and #3: Tampering With and Retaliating Against a Witness in Violation of 18 U.S.C. § 1513(b) and (e) and 18 U.S.C. § 1512(a)(2), (b) and (c)**

178. As described throughout this Complaint, upon information and belief, Defendants Montgomery and Lewis knowingly engaged in conduct whereby they caused damage to Plaintiffs' tangible property, made numerous attempts to cause further damage to Plaintiffs' tangible property, and threatened and incited threats of bodily injury to Tumey and his family.

179. Upon information and belief, this illegal conduct was knowingly engaged in by Montgomery and Lewis against Plaintiffs with the intent to retaliate against Plaintiffs for their



participation in and attendance in official court proceedings related to the pending patent infringement lawsuit filed against Mycroft.

180. Upon information and belief, Defendants Montgomery and Lewis additionally knowingly, and with intent to retaliate, took actions to directly interfere with the lawful employment and livelihood of Plaintiffs, in retaliation for Plaintiffs having provided the Court (as a law enforcement officer) truthful information related to the commission or possible commission of patent infringement by Defendant Mycroft.

181. Upon information and belief, Defendants Montgomery and Lewis made or caused to be made and/or attempted to be made, numerous threats of bodily injury and threats of physical force against Plaintiff Tod Tumey. These threats of bodily injury and physical force were made with the intent to hinder, delay or prevent testimony and/or communications to the Court in an official court proceeding related to the commission or possible commission of a Federal offense by Mycroft (the pending patent infringement action pending against Mycroft).

182. Upon information and belief, Defendants Montgomery and Lewis, acting individually, together or in concert with others, knowingly used intimidation and threats in an attempt to influence, delay or prevent testimony in an official proceeding and to prevent the effective prosecution of pending patent infringement claims asserted against Mycroft.

183. Such actions intentionally harassed Plaintiffs in an attempt to hinder, delay, prevent or dissuade Plaintiffs from continuing the prosecution of the Voice Tech Matters against Mycroft.

184. Defendants Montgomery and Lewis' repeated cyberwarfare attacks against Plaintiffs were made in an attempt to corruptly obstruct, influence or impede an official proceeding.

185. Upon information and belief, Defendants Montgomery and Lewis conspired together and/or in concert with others, to commit the offenses described above in violation of 18 U.S.C. § 1513 and/or 18 U.S.C. § 1512.

**C. RICO Predicate Offense #4: Internet Threats in Violation of 18 U.S.C. § 875**

186. As described throughout this Complaint, upon information and belief, Defendants Montgomery and Lewis, transmitted or caused to be transmitted in interstate commerce, communications containing threats of bodily injury against Plaintiff Tod Tumey. These threats were transmitted with the intent to extort from the Plaintiffs a thing of value (i.e., the dismissal of the pending patent infringement action asserted against Mycroft). *See* Cyberattack Chronology at **Exhibit 7**.

187. Upon information and belief, Defendants committed each of the predicate racketeering activities alleged above willfully and with actual knowledge of the illegal activities.

188. The predicate acts alleged above are related as they have the same or similar purpose, results, participants, victims and methods of commission.

189. By reason and as a result of Montgomery's and Lewis' conduct and participation in the pattern of racketeering activity alleged herein, they have caused damages to Plaintiffs in their business and property.

190. As detailed earlier in the Complaint, such damage includes, but it is not limited to, actual financial loss in the form of employee time spent addressing and responding to hacking attacks, hiring a computer specialist to defend against such attacks, costs associated with increased security (both physical and virtual) at Plaintiffs' offices and home, and the inability to access Plaintiffs property (firm phone lines and email accounts) for the significant periods of time when functionality was entirely shut down due to the volume of cyberattacks.

191. In addition, Defendants' actions employed force, threats of force, fear and/or violence in an attempt to deprive Plaintiffs of their property interest in running their business and continuing to represent and litigate on behalf of their clients.

192. But for the Defendants' racketeering conduct, Plaintiffs would not have been injured as described above.

WHEREFORE, Plaintiffs respectfully demand judgment against Defendants Montgomery and Lewis, for compensatory and treble damages, attorneys' fees and costs, pursuant to 18 U.S.C. § 1964(c), interest, and such other relief as this Court deems just and proper.

**COUNT II**  
**Violation of RICO, 18 U.S.C. § 1962(d) [Conspiracy]**  
**(All Plaintiffs Against Defendants Montgomery and Lewis)**

193. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint

194. This is an action asserted against Defendants Montgomery and Lewis for violation of RICO pursuant to 18 U.S.C. § 1962(d).

195. Upon information and belief, Defendants Montgomery and Lewis were associated with the Mycroft Enterprise and agreed to conspire, in violation of 18 U.S.C. § 1962(d), to invest in, operate, grow, market and sell Mycroft through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(a), to control the Mycroft Enterprise through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(b), and/or to conduct or participate in, directly or indirectly, the conduct and affairs of the Mycroft Enterprise through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c).

196. Upon information and belief, Defendants Montgomery and Lewis knowingly agreed to commit, directly or indirectly, predicate acts of racketeering, namely multiple acts of

wire fraud, tampering with and retaliating against participants in a court proceeding, and internet threats. These are overt acts done by Montgomery and Lewis in furtherance of the conspiracy and to affect the objects thereof, including but not limited to the acts set forth above and outlined in Count III.

197. Upon information and belief, Defendants Montgomery and Lewis have intentionally conspired and knowingly agreed to, directly or indirectly, use or invest income that is derived from a pattern of racketeering activity in an interstate enterprise, acquire or maintain interests in the enterprise through a pattern of racketeering activity, and conduct and participate in the conduct of the affairs of the enterprise through a pattern of racketeering activity. Defendants Montgomery and Lewis knew that their predicate acts were part of a pattern of racketeering activity and agreed to the commission of those acts to further the schemes described above. That conduct constitutes a conspiracy to violate 18 U.S.C. §§ 1962(a), (b), and (c), in violation of 18 U.S.C. § 1962(d).

198. As a direct and proximate result of this conspiracy, the overt acts taken in furtherance of that conspiracy, that were also predicate acts of racketeering activities, and violations of 18 U.S.C. § 1962(d), Plaintiffs were injured in their business and property.

199. Specifically, this damage includes, but it is not limited to, actual financial loss in the form of employee time spent addressing and responding to hacking attacks, hiring a computer specialist to defend against such attacks, costs associated with increased security (both physical and virtual) at Plaintiffs' offices and home, and the inability to access Plaintiffs' property (firm phone lines and email accounts) for the significant periods of time when functionality was entirely shut down due to the volume of cyberattacks.

200. In addition, Defendants actions employed force, threats of force, fear and/or violence in an attempt to deprive Plaintiffs of its property interest in running its business and continuing to represent and litigate on behalf of its clients.

WHEREFORE, Plaintiffs respectfully demand judgment against Defendants Montgomery and Lewis for compensatory and treble damages, attorneys' fees and costs, pursuant to 18 U.S.C. § 1964(d), interest, and such other relief as this Court deems just and proper.

**COUNT III**  
**Violation of the Computer Fraud and Abuse Act ("CFAA") (10 U.S.C. § 1030 *et seq.*)**  
**(All Plaintiffs Against All Defendants)**

201. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

202. Upon information and belief, Defendants, without authorization, knowingly, intentionally and with an intent to defraud, accessed and attempted to access Plaintiffs' protected computers and protected computer network beginning by at least June 1, 2020, and on multiple occasions thereafter. *See* Cyberattack Chronology at **Exhibit 7**.

203. Plaintiffs' computer systems, which the Defendants accessed or attempted to access on numerous occasions, were used to conduct business worldwide and therefore were "used in or affecting interstate or foreign commerce or communication" and meet the definition of a "protected computer" set forth in 18 U.S.C. § 1030(e)(2)(B).

204. Plaintiffs used intricate privacy and security safeguards to insure that the information on their computers and computer systems are restricted to authorized individuals acting within the scope of their authority.

205. Defendants were not authorized to access or use Plaintiffs' protected computers and computer systems.

206. As a result of this intentional unauthorized access, and in violation of 18 U.S.C. § 1030(a)(2)(C), Defendants unlawfully obtained information from Plaintiffs' protected computers and protected computer networks.

207. Further, upon information and belief, through this unlawful conduct, and in violation of 18 U.S.C. § 1030(a)(4), Defendants obtained information of value from Plaintiffs' protected computers without authorization and used such information to further its intended fraud against Plaintiffs.

208. Specifically, as detailed in the paragraphs above, on June 1, 2020, and likely on many other occasions as well, upon information and belief, Defendants accessed Plaintiffs' protected computers, computer systems and computer networks and accessed one or more Tumey L.L.P. email accounts and reviewed the contents of emails. Defendants then used the information found in the illegally accessed email accounts to craft personal, targeted phishing emails to Plaintiff Tumey that would appear legitimate (i.e., that would appear to come from his 12-year-old daughter with the content of a real email containing specific school-related details). **Exhibit 7 at TUMEY000934-936.**

209. In addition, in violation of 18 U.S.C. § 1030(a)(5)(A), upon information and belief, Defendants knowingly caused the transmission of a program, information code or command to Plaintiffs' protected computer which intentionally caused damage to Plaintiffs.

210. Upon information and belief, at the time they engaged in such conduct, both Defendant Montgomery and Defendant Lewis were acting in their own personal interests as well as in the interests of or at the direction of Mycroft.

211. Upon information and belief, Defendants Montgomery and Lewis knowingly conspired to commit a violation of the act.

212. As a result of Defendants' unauthorized, intentional access and attempts to access Plaintiffs' protected computers and protected computer networks, Plaintiffs have suffered damages and a loss of no less than \$5,000 in the last year prior to filing this Complaint, including but not limited to their costs to respond to this offense.

213. Specifically, Defendants' conduct, whether alone or in concert, caused Plaintiffs to incur damages in the form of actual financial loss through lost employee time spent addressing and responding to hacking attacks, hiring a computer specialist to defend against such attacks, costs associated with increased security (both physical and virtual) at Plaintiffs' offices and home, and the inability to access Plaintiffs' property (firm phone lines and email accounts) for the significant periods of time when functionality was entirely shut down due to the volume of cyberattacks.

214. This damage occurred beginning by at least June 1, 2020 and has been ongoing.

215. As a result of the foregoing, Plaintiffs seek their compensatory damages in an amount to be determined at trial.

216. Defendants acted knowingly, willfully, wantonly, maliciously, intentionally, and recklessly in disregarding the rights of the Plaintiffs.

217. Defendants' actions are outrageous, and thus Plaintiffs should be entitled to an award of punitive damages as well.

WHEREFORE, Plaintiffs respectfully pray that this Court enters judgment in favor of Plaintiffs and award them their damages, punitive damages, attorney's fees, costs and all other relief available under the law.

**COUNT IV**  
**Violations of Stored Wire and Electronic Communications Act**  
**(“SCA”), 18 U.S.C. § 2701 *et seq.***  
**(All Plaintiffs Against All Defendants)**

218. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

219. Upon information and belief, Defendants knowingly and intentionally accessed without authorization a facility through which an electronic communication service is provided and thereby gained unauthorized access to Plaintiff’s information. Specifically, through this unauthorized access, Defendants obtained access to an electronic communication while it was in electronic storage.

220. Plaintiffs’ intricate privacy and security safeguards insure that the information on its computer systems and the facility through which Plaintiffs’ electronic communication service is provided is restricted to authorized individuals acting within the scope of their authority.

221. Defendants were not authorized to access or use Plaintiffs’ computer systems and the facility through which Plaintiffs’ electronic communication service is provided.

222. Defendants’ actions also altered or prevented authorized access to electronic communications while the information was in electronic storage.

223. Upon information and belief, Defendants acted willfully and intentionally and therefore, pursuant to 18 U.S.C. § 2707(c), Plaintiffs are entitled to an award of punitive damages as well.

224. Specifically, as detailed in the paragraphs above, on June 1, 2020, and likely on many other occasions as well, Defendants accessed one or more Tumey L.L.P. email accounts and reviewed the contents of emails while they were in electronic storage. Defendants then used the information found in the illegally accessed email accounts to craft targeted phishing emails to



Plaintiff Tod Tumey that would appear legitimate, but were instead designed to do harm to Plaintiffs.

225. Upon information and belief, Defendants Montgomery and Lewis were acting as agents for Defendant Mycroft at the time the above SCA violations were committed.

226. Defendants' actions as described above were in violation of SCA, 18 U.S.C. § 2701(a)(1).

227. Plaintiffs have suffered damages as a result of Defendants' violation of the SCA and seek to recover their actual damages and revenues and/or gains made by Defendants as a result of the violation.

228. Defendants conduct constitutes a willful and intentional violation of the SCA and entitles Plaintiffs to recover exemplary damages pursuant to 18 U.S.C. § 2707(c).

229. Plaintiffs also seek to recover their court costs and reasonable and necessary attorneys' fees for Defendants' violation of the SCA, as described above.

230. While Plaintiffs are seeking an award for their legal damages, there is no adequate remedy at law to fully rectify the actual and prospective loss to Plaintiffs as a result of Defendants' continued misappropriation of their confidential information and documents. The recovery of monetary damages alone cannot prevent the further use or disclosure of the confidential information which Defendants have misappropriated.

WHEREFORE, Plaintiffs pray for judgment against Defendants under Count IV as follows:

- A. Enter a preliminary and permanent injunction requiring Defendants to return all and not retain any copies of information they unlawfully obtained from Plaintiffs;
- B. Award Plaintiffs actual damages in an amount to be determined at trial;

C. Award Plaintiffs punitive damages as a result of Defendants' willful and intentional violation of the SCA;

D. Award attorneys' fees and costs incurred by Plaintiffs in pursuit of this litigation;

E. For further relief the Court deems just and reasonable.

**COUNT V**  
**Tampering with Computer Data Equipment, RS Mo 537.525**  
**(All Plaintiffs Against All Defendants)**

231. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

232. Upon information and belief, one or more of the Defendants, acting individually, together or in concert with others, knowingly, intentionally and without authorization accessed or caused to be accessed Plaintiffs' computer, computer system or computer network.

233. Upon information and belief, one or more of the Defendants, acting individually, together or in concert with others, knowingly, intentionally and without authorization, accessed Plaintiffs' computer, computer system or computer network and took data, programs or supporting documentation residing or existing internal or external to a computer system or computer network in violation of RSMo. 569.095(3).

234. Upon information and belief, one or more of the Defendants, acting individually, together or in concert with others, knowingly, intentionally and without authorization, disclosed or took passwords, identifying code, personal identification numbers, or other confidential information about a computer system or network that is intended to or does control access to the computer system or network in violation of RSMo. 569.095(4).

235. Upon information and belief, one or more of the Defendants, acting individually, together or in concert with others, knowingly, intentionally and without authorization, accessed

computers, computer systems, and/or computer networks, to intentionally examine information about another person in violation of RSMo. 569.095(5).

236. Upon information and belief, one or more of the Defendants, acting individually, together or in concert with others, knowingly, intentionally and without authorization, received, retained, used or disclosed data they knew or believed was obtained in violation of RSMo.569.095(6).

237. Specifically, as described in the paragraphs above, on or about June 1, 2020, Defendants accessed Plaintiffs' computer, computer system or computer network and accessed one or more Tumey L.L.P. email accounts for the express purpose of creating a fraudulent email that would then be sent to Plaintiff Tod Tumey from his daughter's Tumey L.L.P. email address with an imbedded virus. **Exhibit 7 at TUMEY000934-936.**

238. Plaintiffs have been damaged by the above acts, which, upon information and belief, allowed Defendants to access and view email accounts containing highly sensitive privileged material subject to the attorney-client privilege, but to also find personal information in such email accounts (such as the name and email address of Tumey's daughter) and craft fraudulent phishing emails purporting to be from Tumey's daughter which were embedded with sophisticated viruses intended to harm and attack Plaintiffs even further.

239. Plaintiffs seek their compensatory damages as allowed by statute, including but not limited to lost profits, and/or actual, non-economic and/or economic damages suffered by them.

240. Plaintiffs have been forced to incur attorney's fees to prosecute this claim and are therefore entitled to recover their attorney's fees and costs pursuant to RSMo. 537.525(2).

**COUNT VI**  
**Breach of Computer Security, Tex. Civ. Prac. & Rem. Code § 143.001 *et seq.***  
**(All Plaintiffs Against All Defendants)**

241. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

242. This cause of action is brought by Plaintiffs against Defendants pursuant to the Texas Harmful Access by Computer Act, Tex. Civ. Prac. & Rem. Code 143.001 *et. seq.*

243. Upon information and belief, on numerous occasions, Defendants, acting individually, together or in concert with others, knowingly and intentionally accessed a computer, computer network or computer system without the effective consent of the owners, the Plaintiffs, in violation of Section 33.02 of the Texas Penal Code.

244. Upon information and belief, Defendants' unauthorized access to Plaintiffs' computer, computer network or computer system was done with the intent to defraud or harm another or alter, damage or delete the property the Defendants' knowingly accessed

245. Plaintiffs have been injured by Defendants knowing and intentional access to Plaintiffs' computers, computer networks, and computer systems without consent. Specifically, Defendants' conduct, whether alone or in concert, caused Plaintiffs to incur damages in the form of actual financial loss through lost employee time spent addressing and responding to hacking attacks, hiring a computer specialist to defend against such attacks, costs associated with increased security (both physical and virtual) at Plaintiffs' offices and home, and the inability to access Plaintiffs' property (firm phone lines and email accounts) for the significant periods of time when functionality was entirely shut down due to the volume of cyberattacks.

246. Upon information and belief, Defendants acted knowingly, willfully, wantonly, maliciously, intentionally, and recklessly in disregarding the rights of the Plaintiffs.

247. Defendants' actions are outrageous, and thus Plaintiffs should be entitled to an award of punitive damages as well.

248. Defendants Montgomery and Lewis were employed in a managerial capacity and acting with the scope of employment at the time these violations occurred.

249. Plaintiffs are entitled to recover their actual damages for injuries caused by Defendants' knowing and intentional access to Plaintiffs' computer, computer network or computer system without consent. Tex. Civ. Prac. & Rem. Code § 143.002(a).

250. Plaintiffs are also entitled to recover punitive damages against Defendant Mycroft as the employer for the intentional violations caused by its managerial employees acting within the scope of employment.

251. Plaintiffs are also entitled to recover their reasonable attorneys' fees and costs for bringing this action. Tex. Civ. Prac. & Rem. Code § 143.002(b).

**COUNT VII**  
**Intrusion on Seclusion**  
**(Plaintiff Tumey Against All Defendants)**

252. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

253. Upon information and belief, Defendants, through conduct described throughout this Complaint, intentionally intruded upon Plaintiff Tumey's solitude, seclusion, private affairs and concerns by unlawfully accessing Plaintiffs' computers, computer systems or computer networks, accessing and reviewing Tumey's emails, and engaging in harassing and threatening hacking activities directed at Tumey's immediate family, including his wife and minor children.

254. Specifically, upon information and belief, Defendants unlawfully accessed Tumey's emails and reviewed private communications sent between Tumey and his family

members. Defendants then utilized those private emails to craft fraudulent phishing emails embedded with sophisticated viruses, so that it would appear to Tumey that the email was actually coming from his daughter.

255. Plaintiff Tumey had a reasonable expectation of privacy in email communications that were sent.

256. Additional conduct by the Defendants that constitutes an intrusion on Plaintiff Tumey's solitude, seclusion, private affairs and concerns includes repeated hacking attempts on his wife and children, crude and violent threats of bodily injury, and harassing comments and threats directed at his children.

257. The conduct described above would be highly offensive to a reasonable person.

258. Upon information and belief, Defendants acted with intent and malice in the conduct described above.

259. As a result of Defendants' conduct, Plaintiff Tumey has suffered and will continue to suffer damages, including mental and emotional distress.

260. Defendants acted intentionally and maliciously in targeting Plaintiff Tumey's wife and daughter, and in maliciously sending repeated threats of physical harm to Tumey.

261. Defendants' actions were done with the intent to cause Plaintiff Tumey severe mental anguish and distress such that he would feel compelled to drop the prosecution of the patent infringement lawsuit against Mycroft.

262. Plaintiff seeks punitive and/or exemplary damages.

263. While Plaintiff seeks an award for his legal damages, there is no adequate remedy at law to full rectify the actual and prospective harm to Plaintiff and his family as a result of Defendants' continued conduct.

264. Thus, Plaintiff additionally seeks the entry of a temporary, preliminary, and permanent injunction requiring Defendants to refrain from any and all further cyberattacks, harassment and threats directed at Plaintiff Tumey, his immediate family, and his law firm Tumey L.L.P.

**COUNT VIII**  
**Tortious Interference with Business Expectancy**  
**(All Plaintiffs Against All Defendants)**

265. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

266. As a result of long-standing business and commitment to customer service, Plaintiffs have developed an excellent reputation in the industry for the legal services they offer and have developed repeat customers for which they have a reasonable valid business expectancy and probable future business relationships.

267. Defendants were aware of the nature of Plaintiffs' business, their relationships and valid business expectancies.

268. Without justification, upon information and belief, Defendants intentionally interfered with this valid business expectancy through the campaign of information warfare targeted at Plaintiffs and described throughout this Complaint, all of which disrupted Plaintiffs' business and injured Plaintiffs' business reputation.

269. Defendants' acts were not justified and caused Plaintiffs' damages, including lost revenue.

270. Defendants' conduct was outrageous such as to constitute evil motive or reckless indifference to Plaintiffs' rights, warranting an award of punitive damages.

271. While Plaintiffs seek an award for his legal damages, there is no adequate remedy at law to fully rectify the actual and prospective harm to Plaintiffs as a result of Defendants' continued conduct, including the ongoing injury to Plaintiffs' good will and reputation, and continued loss of clients and business expectancies.

WHEREAS, Plaintiffs respectfully request the Court enter judgment against Defendants and in favor of Plaintiffs and award injunctive relief to prevent continued irreparable harm, money damages to compensate it for the harm caused by Defendants, punitive damages that are fair and reasonable yet will serve to deter Defendants from similar conduct in the future, and any other relief the Court deems just and proper.

**COUNT IX  
ASSAULT  
(PLAINTIFF TUMEY AGAINST ALL DEFENDANTS)**

272. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

273. Upon information and belief, one or more Defendants, acting individually, together or in concert with others, intentionally or knowingly threatened Plaintiff with imminent bodily injury or offensive contact.

274. Upon information and belief, Defendants made the unlawful threats with the apparent present ability to effectuate and carry out such threats and attempts into effect.

275. Upon information and belief, Defendants' conduct was undertaken with specific intent to cause Plaintiff fear or apprehension of imminent peril or other physical harm.

276. Plaintiff experienced apprehension of bodily harm or offensive contact as a result of Defendants' conduct.



277. As a result of Defendants' conduct, Plaintiff was harmed, including by experiencing mental and emotional anguish and suffering.

278. Upon information and belief, Defendants acted with intent and malice in the conduct described above.

279. Defendants acted intentionally and maliciously in targeting Plaintiff Tumey's wife and children, and in maliciously sending repeated threats of physical harm to Tumey.

280. Plaintiff seeks punitive and/or exemplary damages.

281. While Plaintiff seeks an award for his legal damages, there is no adequate remedy at law to fully rectify the actual and prospective harm to Plaintiff and his family as a result of Defendants' continued conduct.

282. Thus, Plaintiff additionally seeks the entry of a preliminary and permanent injunction requiring Defendants to refrain from any and all further cyberattacks, harassment and threats directed at Plaintiff Tumey, his immediate family, and his law firm Tumey L.L.P.

**COUNT X**  
**INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS**  
**(Plaintiff Tumey Against All Defendants)**

283. Plaintiffs incorporate by reference as if fully restated herein its allegations contained in all of the foregoing Paragraphs of this Complaint.

284. Upon information and belief, through the campaign of targeted information warfare and cyberattacks described herein, including through threats to Plaintiff's family and young children, Defendants acted intentionally or recklessly to cause Plaintiff extreme emotional distress.

285. Defendants' conduct was extreme and outrageous in character, going beyond all bounds of decency as to be regarded as atrocious and utterly intolerable in a civilized community.

286. Upon information and belief, Defendants' actions were done with the intent of causing actual emotional distress and harm to Plaintiff and members of his family.

287. Plaintiff has experienced extreme emotional distress as a result of Defendants' conduct.

288. Defendants' conduct was outrageous such as to constitute evil motive or reckless indifference to Plaintiff's rights, warranting an award of punitive damages.

289. While Plaintiff seeks an award for his legal damages, there is no adequate remedy at law to full rectify the actual and prospective harm to Plaintiff and his family as a result of Defendants' continued conduct.

290. Thus, Plaintiff additionally seeks the entry of a preliminary and permanent injunction requiring Defendants to refrain from any and all further cyberattacks, harassment and threats directed at Plaintiff Tumey, his immediate family, and his law firm Tumey L.L.P.

### **Jury Demand**

Plaintiffs demand a trial by jury upon all issues raised in this Complaint.

### **Prayer for Relief**

1. For the forgoing reasons, Plaintiffs respectfully request that they be granted the following relief:

- a. Entry of a preliminary injunction, thereafter to be made permanent, that, among other things, enjoins Defendants from engaging in or intentionally inciting any cyberattacks, hacking or other harassment directed at Plaintiffs and Plaintiff Tumey's immediate family members, and granting all other injunctive relief requested herein and as may be warranted to protect Plaintiffs;
- b. Judgment in favor of Plaintiffs on Counts I through X;

- c. Award of compensatory damages, disgorgement of revenues and/or gains wrongfully acquired, treble damages and other statutory relief available, and an award of punitive / exemplary damages;
- d. Entry of an order directing Defendants to return all copies of Plaintiffs' information or documents that may have been obtained by Defendants through their unauthorized access to Plaintiffs' computer systems;
- e. Enter of an order directing Defendants to identify any person or persons to whom any information or documents obtained from their unauthorized access to Plaintiffs' computer systems may have been disclosed;
- f. Award of reasonable attorneys' fees and the costs of prosecuting this action;
- g. Award pre- and post-judgment interest on damages as allowed by law; and
- h. An award to Plaintiffs of all other relief, in law and in equity, to which they may show itself to be entitled or as the Court deems just and appropriate.

Dated: February 24, 2021.

Respectfully submitted,

**BERKOWITZ OLIVER LLP**

By: /s/ Stacey R. Gilman

Stacey R. Gilman (MO Bar #55690)

Lauren Tallent (MO Bar # 72304)

2600 Grand Boulevard, Suite 1200

Kansas City, Missouri 64108

(816) 561-7007

(816) 561-1888 *fax*

[sgilman@berkowitzoliver.com](mailto:sgilman@berkowitzoliver.com)

[ltallent@berkowitzoliver.com](mailto:ltallent@berkowitzoliver.com)

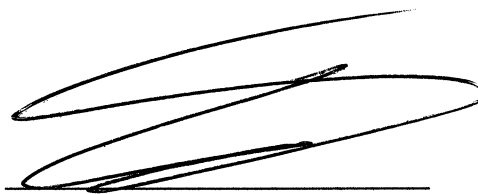
**ATTORNEYS FOR PLAINTIFFS TOD TUMEY AND  
TUMEY L.L.P.**

## VERIFICATION

I, Tod T. Tumey, declare as follows:

1. I am a Plaintiff in the present case and a citizen of the United States of America.
2. I have reviewed the Complaint and believe all of the allegations to be true.
3. I have personal knowledge of myself, my activities, my intentions, and the harassment I experienced, including the facts set out in the forgoing *Verified Complaint*, and if called upon to testify I would competently testify as to the matters stated herein.
4. I have personal knowledge of my law firm, Tumey L.L.P., its activities, its business, and the harassment it experienced, including the facts set out in the forgoing *Verified Complaint*, and if called on to testify I would competently testify as to the matters stated herein.
5. I verify under penalty of perjury under the laws of the United States of American that the factual statements in this *Complaint* concerning myself, my activities, and my intentions are true and correct, as are the factual statements concerning Tumey L.L.P., its activities, its business and its intentions. 28 U.S.C. § 1746.

Executed On February 22, 2021.

A handwritten signature in black ink, consisting of several loops and a horizontal line at the bottom, positioned above the printed name.

Tod. T. Tumey